

# Privacy Practices for Competitive Advantage

April 07, 2008

David A. VanderNaalt

[www.azgita.gov/sispo](http://www.azgita.gov/sispo)

*Privacy is the goal*

*Security is the journey*

*Technology can help*

*People are the key*



# Agenda

- SISPO introduction
- Executive Order 2008-10
- Things you can do
- Future



# David VanderNaalt – BIO Highlights

- Arizona's Chief Information Security Officer
  - Governor announced appointment Sept. 05, 2007
  - Appointed September 17, 2007
    - Head Statewide Information Security & Privacy Office
- NYC Dept. of Investigation 1999-2007
  - Director Citywide Information Security (CISO)
  - Director Digital Crimes Investigation Unit
  - Director Citywide Continuanace Planning (OEM)
  - Yes → 09-11-01
- American Express, World Wide 1985-1996
  - Corporate Information Security Officer (1989)
  - *Ponemon Institute; Distinguished Fellow*
  - *Certified Information Security Manager*



# Mary Beth Joubland – BIO Highlights

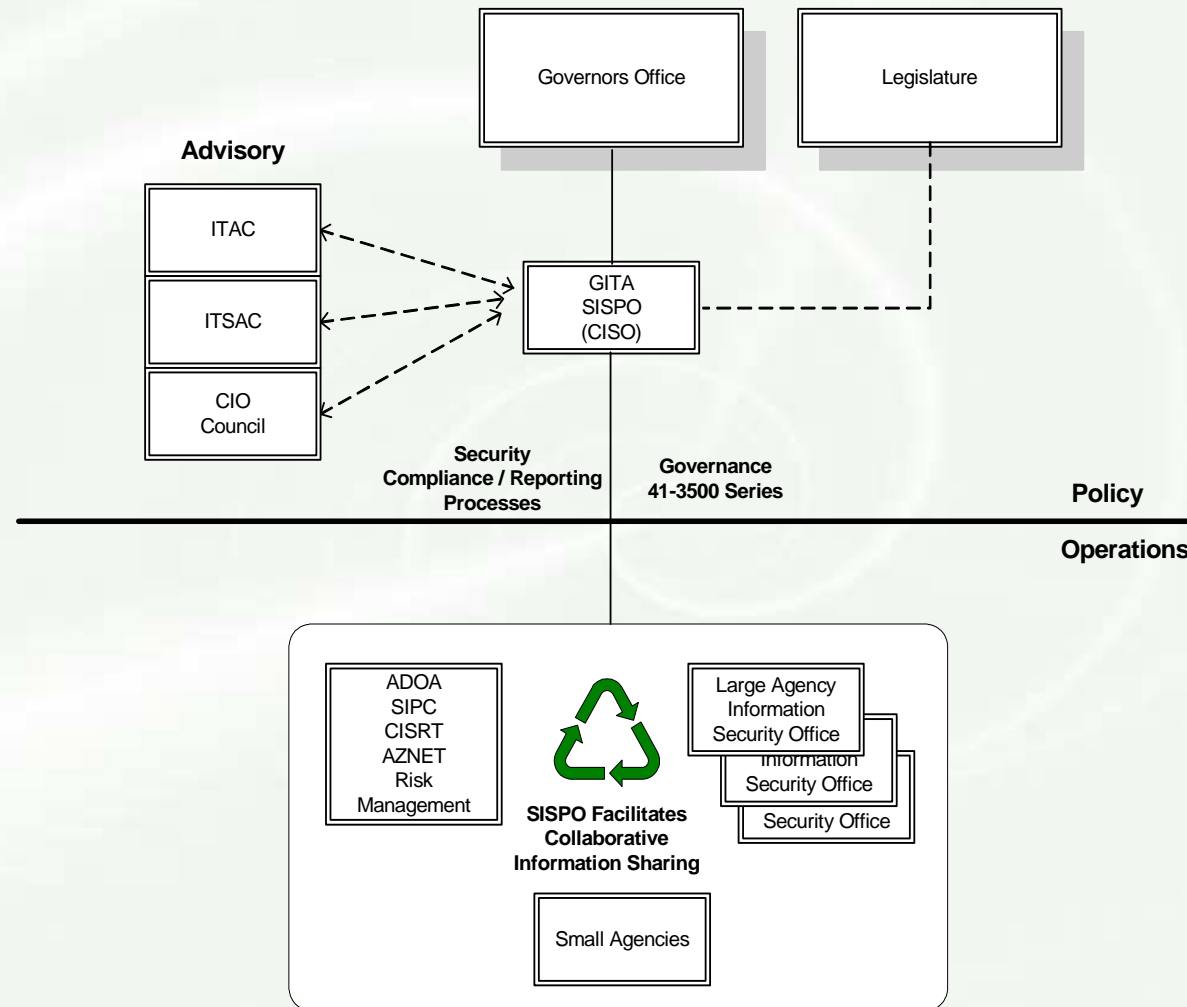
- Arizona's Chief Privacy Officer
  - Appointed January 15, 2007
  - Licensed AZ Attorney & member of AZ State Bar
- Chief Health Insurance Portability and Accountability Act (HIPAA) Compliance Officer (ADHS)
  - Created HIPAA Privacy and Security compliance program
  - Member of the Statewide HIPAAZ Workgroup
  - Chairperson Human Subjects Research Review Board
- Appointee to National Academy of Science, Institute of Medicine Committee on HIPAA and Research



# The Statewide Information Security & Privacy Office resides within the Government Information Technology Agency



# SISPO Organizational Framework



# A.R.S. 41-3501 et. seq.

## GITA's Roles and Responsibilities

- Establish Statewide IT Policies & Standards
  - Develop / Monitor compliance
  - Includes Information Security & Privacy
- Statewide Coordinator IT projects
- Evaluate Agency IT Plans
- Develop & Implement a Statewide IT Plan
- Inventory IT Assets of the State
- Oversight Agency IT Projects (\$25k - \$1M+)
  - Project Investment Justification (PIJ)
  - Information Technology Authorization Committee
    - \$1M→ITAC
  - Approve / Disapprove / Suspend
- No operations





# A.R.S. 41-3507

## SISPO's Roles and Responsibilities

- Strategic planning & coordination
- Individual budget units continue operations
- Compliance plan for InfoSec & Privacy
- Temporarily suspend information infrastructure
- Agency required to report incidents
  - Coordinate
  - Review
  - Mitigation
- Training & Awareness Program
  - Web based e-Learning
  - Leverage already in place programs





# A.R.S. 41-3507

## **41-3507. Statewide information security and privacy office; duties; suspension of budget unit's information infrastructure**

A. The statewide information security and privacy office is established in the government information technology agency. The statewide information security and privacy office shall serve as the strategic planning, facilitation and coordination office for information technology security in this state. Individual budget units shall continue to maintain operational responsibility for information technology security.

B. The director shall appoint a statewide chief information security officer to manage the statewide information security and privacy office. The statewide chief information security officer shall report to the director pursuant to section 41-3503.

C. The statewide information security and privacy office shall develop, implement, maintain and ensure compliance by each budget unit with a coordinated statewide assurance plan for information security and privacy. The statewide information security and privacy office shall:

1. Direct information security and privacy protection compliance reviews with each budget unit to ensure compliance with standards and effectiveness of security assurance plans as necessary.
2. Identify information security and privacy protection risks in each budget unit and direct agencies to adopt risk mitigation strategies, methods and procedures to lessen these risks.
3. Monitor and report compliance of each budget unit with state information security and privacy protection policies, standards and procedures.
4. Coordinate statewide information security and privacy protection awareness and training programs.

5. Develop other strategies as necessary to protect this state's information technology infrastructure and the data that is stored on or transmitted by such infrastructure.

D. The statewide information security and privacy office may temporarily suspend operation of information infrastructure that is owned, leased, outsourced or shared in order to isolate the source of, or stop the spread of, an information security breach or other similar incident. A budget unit shall comply with directives to temporarily discontinue or suspend operations of information infrastructure.

E. Each budget unit and its contractors shall identify and report security incidents to the statewide information security and privacy office immediately on discovery and deploy mitigation strategies as directed.



# SISPO Team

- Chief Information Security Officer (SISPO)
- Chief Privacy Officer (SISPO)
- Manager Awareness & Training (SISPO)
- Manager IT Homeland Security (GITA)
- Future
  - Compliance Reviews
  - Vulnerability and Threat Assessments
  - Incident Response Coordination
  - COOP Consulting (EPOC / State COOP / Tech DRP)



# SISPO Activities

- Review Incidents
  - Direct and coordinate
  - Internal controls & procedures
- Fulfill the Mandate of Executive Order 2008-10
  - Scorecard
- Update Cyber Terrorism response plan
  - Governor's Playbook
  - AZ Incident Response (planning)
- Update Incident Reporting Procedures
- Policy & Standards
  - Review/update & formulate new
- TISA (Technology Infrastructure & Security Assessment)
  - Annual & year over year trend reporting
- Project Investment Justification (PIJ)
  - Update: Security / Privacy / Recovery



# SISPO Activities

- Developing employee certifications
  - AZ Certified InfoSec Practitioner
  - AZ Certified Privacy Practitioner
- Developing online incident reporting
  - Framework / tree
- Health-e Connections
  - Privacy sub-committee
  - Security sub-committee
- Developing Privacy Assessment
  - Annual & year over year trend reporting
- Developing an annual conference
- Statewide Risk Assessment



# SISPO Relationships

## ❖ Ongoing Interactions

- Governor's Cabinet
- Agency executives
- Agency CIOs
- Agency CISOs
- Agency CPOs
- Legislators
- Committees
- Other branches of AZ Gov't
- Other state CISOs & CPOs

## ❖ Communicate

- G1 Deputy Directors
- G2 Directors
- Agency CIOs
- Agency POs
- Agency ISOs

## ❖ Universities

## ❖ Key Industry Groups

## ❖ Leading Companies



# Identity theft prevention

- ↪ SISPO is focused on information protection
- ↪ Creating a state level workgroup
  - ① Law enforcement
  - ① Attorney General Office
  - ② Privacy Officers
  - ③ Private companies
  - ③ Service providers
- ↪ New web page for ID Theft resources





Identity theft refers to crimes involving illegal usage of another individual's identity. The most common form of identity theft is credit card fraud. According to the non-profit [Identity Theft Resource Center](#), identity theft is sub-divided into four categories:

- The following resources are Federal efforts protecting from Identity Theft:

- Important information from the Federal Trade Commission, the nation's consumer protection agency:** [annualcreditreport.com](https://annualcreditreport.com) is the **ONLY** authorized online source for you to get a free credit report under federal law. You can get a free report from each of the three national credit reporting companies every 12 months. Some other sites claim to offer "free" credit reports, but may charge you for another product if you accept a "free" report.

- ### General Information on Identify Theft

- one



# EO 2008-10

- EO covers
  - All State Executive Branch agencies
  - Expectation: others comply → best practice
- January 14, 2008
- WHEREAS;
  - Prevention cheaper than mitigation
  - Protect citizen information



# EO 2008-10

Each Agency shall:

1. Appoint Agency ISO = Technology
2. Appoint Agency PO = Business (note option)
3. Work with SISPO to develop protections
  - Digital
  - Paper
4. Deploy encryption
  - RFP completed (HB 2785 Section 23)
    - GITA Notice of Intent (NOI)
5. Telecommute procedures
  - Proper physical & logical security



# EO 2008-10

6. Redaction procedure (ARS 41-4172)
7. Report all incidents (S855)
  - Any information loss or mis-use
  - Any technology infrastructure attack
8. Data breach notification procedure (ARS 44-7501)
9. Physical security
10. Training & Awareness programs
  - Privacy
  - Information Security



# Things you can do

## ☐ Develop relationships

- Information Security
- Privacy Office
- General Counsel
- Corporate Compliance
- Procurement
- Risk Management
- Audit
- Physical Security
- Law enforcement
- Chief Operating Officer
- Marketing – information broker
- Leader Technology



# Things you can do

- ☐ Define Policy & Standards
- ☐ Awareness Program
- ☐ Lock up laptops (not trunk / back seat)
  - Specific procedure for handling information in transit
- ☐ Gather metrics
  - Assessment
  - Compliance
- ☐ Encrypt Encrypt Encrypt (MBJ)
- ☐ Information Inventory
- ☐ Secure paper documents



# Future Asset Protection

- o Merging of protection functions
  - Last 5 years - CSO
    - Information Security
    - Physical Security
- o Make InfoSec/Privacy strategic
  - ✓ Put operations back in operations
    - Ex: management of firewalls
  - Security operations group
- ➔ Senior Executive
  - All asset protection functions



# Future Asset Protection

## Asset protection – Senior Executive

- Privacy
- Information Security
- Technology Infrastructure protection
- Physical security
- Risk Management
- Legal compliance  
(local/state/federal/international)
- External investigation
- Internal investigation





# Remember

**Privacy is the GOAL**


**Security is the journey**

**Technology can help**

**People are the key**



# Children & Computers

 Would you allow your child at night to walk down a street alone to get to the library:

- Pimps / prostitutes
- Drug pushers / users
- No street lights
- No police
- Halfway house for released pedophiles
- Porn magazines laying in the street

- ✓ Porn largest industry on the INTERNET
- ✓ Chat rooms are un-monitored
- ✓ Social sites – little/no oversight



# Children & Computers

## Actions/Monitoring/Filtering

- ☐ **Talk/explain**
- ☐ **Computer(s) in open space – family/front room never bedroom**
- ☐ **Browser security**
- ☐ **ISP controls**
- ☐ **Kids control sftwre**
- **MONITOR!!!**
- ✓ **Combination security package**
  - Firewall
  - AntiVirus
  - Email scan
  - Spam
  - Popup
  - Spyware
  - Phishing
  - Filtering



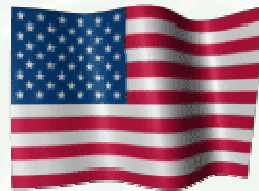
# Children & Computers

**Remember:  
the bad guy only has to be  
successful once**



From a veteran

to every member of the  
U.S. Armed Forces



and their families

**THANK YOU**



# Contact

**David A. VanderNaalt**

Chief Information Security Officer

State of Arizona

Statewide Information Security & Privacy Office

<http://azgita.gov/sispo/>

Government Information Technology Agency

100 N. 15th Ave. Suite 440

Phoenix, Arizona 85007

602.364.0535

[dvandernaalt@azgita.gov](mailto:dvandernaalt@azgita.gov)

